

Requested Patent: WO0147177A1

Title:

ENCRYPTION OF PROGRAMS REPRESENTED AS POLYNOMIAL MAPPINGS AND  
THEIR COMPUTATIONS ;

Abstracted Patent: WO0147177 ;

Publication Date: 2001-06-28 ;

Inventor(s): BREKNE TOENNES (NO) ;

Applicant(s): BREKNE TOENNES (NO); TELENOR AS (NO) ;

Application Number: WO2000NO00438 20001220 ;

Priority Number(s): US19990172572P 19991220 ;

IPC Classification: H04L9/28 ; G06F17/10 ;

Equivalents: AU2716701

ABSTRACT:

Three variations of a method of representing (abstract) state machines as polynomial mappings, and three variations of a corresponding encryption program stored on a computer readable medium. The encryption program is based directly on symbolic functional composition of polynomial mappings with permutations expressed as polynomial mappings.

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number  
**WO 01/47177 A1**

- (51) International Patent Classification<sup>7</sup>: H04L 9/28, G06F 17/10 (74) Agent: BRYN & AARFLOT AS; P.O. Box 449 Sentrum, N-0104 Oslo (NO).
- (21) International Application Number: PCT/NO00/00438 (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (22) International Filing Date:  
20 December 2000 (20.12.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
60/172,572 20 December 1999 (20.12.1999) US (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (*for all designated States except US*): TELENOR AS [NO/NO]; P.O. Box 6701 St. Olavsplass, N-0130 Oslo (NO). Published:  
— With international search report.
- (72) Inventor; and
- (75) Inventor/Applicant (*for US only*): BREKNE, Tønnes [NO/NO]; Jonsvannsveien 93A, N-7050 Trondheim (NO). For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 01/47177 A1

(54) Title: ENCRYPTION OF PROGRAMS REPRESENTED AS POLYNOMIAL MAPPINGS AND THEIR COMPUTATIONS

(57) Abstract: Three variations of a method of representing (abstract) state machines as polynomial mappings, and three variations of a corresponding encryption program stored on a computer readable medium. The encryption program is based directly on symbolic functional composition of polynomial mappings with permutations expressed as polynomial mappings.